

Cisco Application-Oriented Networking 3.0

Product Overview




The Cisco® Application-Oriented Networking (AON) platform is the industry pioneer of the class of products that facilitate application-fluent networks based on highly distributed, service-oriented, and legacy architectures. Cisco AON continues to embed application intelligence into the network to better meet the underlying needs of applications for multi-enterprise security, real-time visibility, event-driven messaging, optimized delivery, and other core integration and deployment services.

The AON 3.0 release is the next generation of the AON platform and includes many new features such as automatic Policy Execution Plan (PEP) generation for enrichment and enforcement of policies specified within Web Services Description Language (WSDL) and Web Services Policy Framework (WS-Policy) artifacts, a new Create SOAP Message bladelet for Web Services callouts, Security Assertion Markup Language (SAML) 2.0 support, HTTP pipelining, data streaming support, and extensive Simple Network Management Protocol (SNMP) MIB metrics, to name a few. The complete list of new features in AON 3.0 is in Table 5.

Unlike other application-fluent network devices, Cisco AON distinguishes itself by being the most flexible and programmable. It has multiple development kits that allow customers to add their own business logic and apply these as network policies to incoming and outgoing traffic based on application business rules. In addition, it is the only such system, in its category, that may operate in a promiscuous mode, if the desire is primarily to monitor application traffic and function in an out-of-band manner rather than in-line.

AON is available in multiple form factors, which can be selected based on the customer's topological and performance requirements. These form-factors are shown in Figure 1.

Figure 1. Cisco AON Form Factors

Branch Office		Enhanced Network Module for Cisco 2800/3700/3800 Routers Single-core 1 GHz Intel 373 Celeron-M CPU, 1 GB RAM, 80 GB hard disk drive
		CADE-1010 Integrated Single-Core Appliance Single-core Intel D352 3.2 GHz CPU, 1 GB RAM, 250 GB hard disk drive
Enterprise Data Center		CADE-2142 Integrated Dual Quad-Core Appliance 2 Quad-Core Intel E5320 1.86 GHz CPUs. Up to 4 GB RAM; 2x147 GB hard disk drive

Features and Benefits

Cisco AON natively understands the content and context of application messages (for example, a purchase order or a stock trade), and conducts operations on those messages in-flight according to business-driven policies and rules. Cisco AON delivers this breakthrough level of application intelligence to complement and extend Cisco integrated network services technologies, resulting in a new level of immediate and deep insight for making real-time business decisions.

Cisco AON complements existing networking and application technologies with enhanced security, visibility, messaging, and optimization services that provide a higher degree of awareness regarding essential business information flowing in the network. These services help to:

- Enforce consistent business policies across information access and exchange
- Provide visibility of information flow, including monitoring and metering of information flow for both business and infrastructure purposes
- Facilitate communication between disparate applications by routing information to the appropriate destination, in the format expected by that destination
- Enhance application optimization by providing application-level load-balancing, processing offload, message caching, and compression services

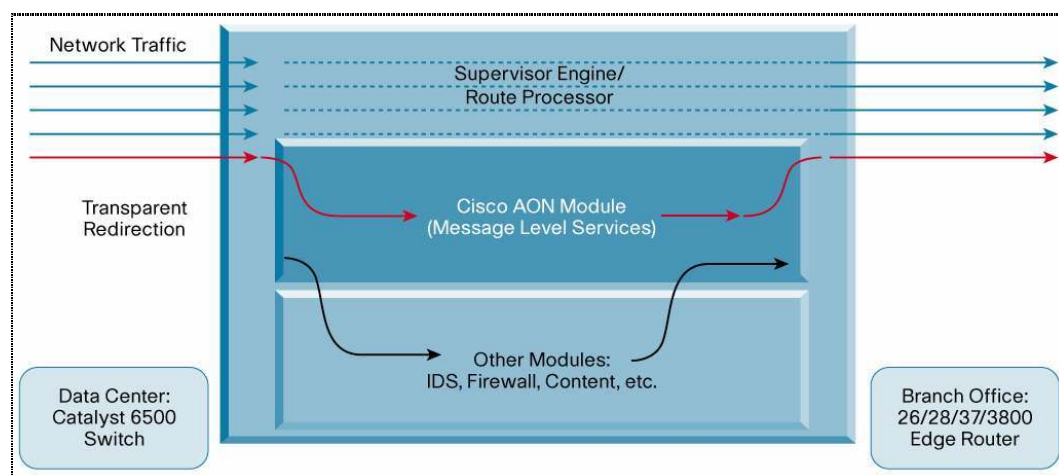
Cisco AON works primarily at the message level rather than the packet level. Typically it inspects the full message, including the payload as well as all headers. It also understands and enhances delivery of application-level protocols such as HTTP and Java Messaging Service (JMS).

Core messaging and other baseline application services have typically been developed using application software and expensive custom code. Instead, Cisco AON creates a pervasive, intelligent network to provide these capabilities, helping realize significant business gains in terms of:

- Embedded awareness that spans applications and computing environments
- Real-time business information that informs and facilitates rapid yet precise decision making
- Network-guided optimization that boosts application performance and reliability

Cisco AON Operation

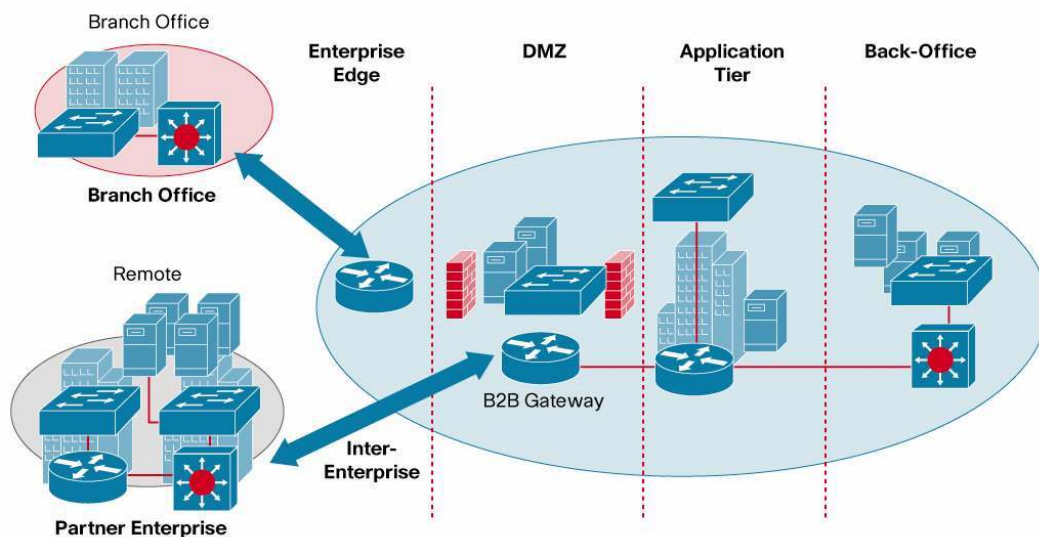
The supervisor engine or route processor in a switch or router can transparently redirect application traffic to a Cisco AON device (blade or appliance) without requiring any changes to the applications themselves (Figure 2). Policies can then be applied to these messages and forwarded to the destination application. Cisco AON also can be explicitly addressed if required.

Figure 2. Traffic Redirection to AON

The following tools are available to configure and manage these devices:

- Cisco AON Development Studio (ADS) is used to create Policy Execution Plans (PEPs) that represent a set of operations (bladelets) to apply to application messages.
- Cisco AON Management Console (AMC) provides centralized control for configuration, certificate management, and lifecycle management of a distributed AON network.

The Cisco AON platform helps enable a wide range of usage scenarios across an application network (Figure 3).

Figure 3. AON Deployment Usage Scenarios

Following are some scenarios in which Cisco AON is typically deployed.

- **In the remote office or business-to-business (B2B) spoke:** Cisco AON devices can be deployed for infrastructure consolidation. A single device can provide all the services required by the branch to effectively communicate with the central office. Cisco AON helps enable these services by bridging disparate applications and optimizing network usage at the application level. Cisco AMC provides centralized management for distributed branch-office deployment of application policies.
- **At the enterprise edge:** Cisco AON can act as an application-security gateway or a B2B gateway. As an Extensible Markup Language (XML) trust enforcement point, it provides consistent authentication, authorization, and accounting (AAA) enforcement across all backend services and applications. As a B2B gateway, Cisco AON helps enable a transparent interface with trading partners by providing trust, policy enrichment and enforcement, protocol bridging, and message validation and transformation services.
- **At the enterprise core:** Cisco AON provides transparent interapplication communication, and it can intercept and analyze traffic in message formats such as XML. It also provides a network-embedded communication bridge between protocols and applications. Cisco AON helps applications offload infrastructure functions such as message-level load balancing to the network, where they can scale effectively.

AON Features

Security

To enforce application security policy within the network, Cisco AON provides a set of services that help enable message-level access and control.

- **Authentication:** Cisco AON can verify the identity of a sender's inbound message-based content (username and password, WS-Security [WSS] profile, digital certificate, and so on). The solution integrates with security frameworks, such as Kerberos Protocol, and Lightweight Directory Access Protocol (LDAP) servers such as Netegrity SiteMinder, Microsoft Active Directory, OpenLDAP, and SunONE.
- **Authorization:** Cisco AON can determine which level of access the originator of the message should have to the services it is attempting to invoke. Features supported include SAML Authorization Assertion embedded in SOAP, WSS headers, LDAP group-based authorization, and customer-defined rule-based control policies.
- **Non-repudiation and data integrity:** Cisco AON can digitally sign message elements or entire messages at any given AON device. Features supported include insertion and verification of XML signatures in WSS headers, detached envelope and enveloping XML signature types, signatures based on private keys, SHA-1 digest computation, and RSA digest encryption.
- **Confidentiality:** Based upon policy, Cisco AON can encrypt and decrypt message elements or entire messages. Features supported include Triple Digital Encryption Standard (3DES) and Advanced Encryption Standard (AES)-128/192/256 symmetric ciphers, RSA symmetric ciphers, destination URL-based keys, and certificates.

- **Centralized key management:** Cisco AMC allows users to register, configure, bind, and provision keys and certificates from the Cisco AMC server to the AON device. Capabilities include generating, registering, and obtaining Class 2 and Secure Sockets Layer (SSL¹) certificates using Verisign Class 3 Certificate Service; fetching, uploading, and importing SSL certificates; importing PKCS#12 certificates; and importing keys from Java keystores.
- **Transport-layer security:** Cisco AON supports transport-layer security mechanisms such as TLS 1.0 and SSL 3.0.

Visibility

Each Cisco AON node can be configured to act as a sensor that captures, processes, and logs highly granular information about application messages. This capability helps Cisco AON provide an event-capture fabric for specified application messages. Cisco AON can inspect the messages and apply rules at the message-content level.

- **Out-of-band message processing through promiscuous mode:** Cisco AON can receive and process messages without increasing latency in network traffic, helping enable out-of-band monitoring and analysis. For example, Financial Information eXchange (FIX) Protocol and HTTP sessions are received out of band, assembled to recreate the messages, then appended with relevant metadata such as time stamps and relevant TCP headers. These messages can be used to analyze scenarios such as transaction monitoring, intrusion detection, insider threats, or FIX monitoring. And service-level agreement (SLA) customers can take advantage of the extensibility framework to tap and frame their proprietary message formats.
- **Logging:** Cisco AON can log messages to external systems for purposes of auditing and compliance or for future analysis.
- **Contextual lookup:** Cisco AON can refer to external systems to obtain contextual information required to analyze the data. For example, it can call out to a customer database to look up customer priority based on a customer ID in the message.
- **Notification and alerting:** Cisco AON can notify or alert other applications in case of an abnormal event. For example, if an SLA time to deliver a message has not been fulfilled, operations personnel can be alerted to take corrective action.

Intelligent Message Routing

Given its role as an intermediary in highly heterogeneous application environments, Cisco AON must flexibly adapt to different types of enterprise information, business policies, and endpoints. Cisco AON operates at the application-message level, allowing a high degree of flexibility:

- **Application quality of service (AppQoS):** The AppQoS feature helps Cisco AON users set application message- and transaction-level priorities and align them with network-level QoS capabilities. For example, an enterprise SAP system can be made to process purchase orders with a higher priority than price quotes and enforce that priority across the application infrastructure and the network. The priorities map to network QoS functions, which in turn direct the priority of message processing both within the AON node and at the transport level in the network. The business result is better alignment of IT infrastructure usage with a higher degree of automatic SLA enforcement, even in times of severe network congestion.

¹ This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more details please visit the following website: <http://www.openssl.org/>.

- **Protocol support:** Cisco AON understands various application access methods and provides adapters for most commonly used protocols: HTTP, HTTPS, Tibco EMS, WebSphere JMS and MQ, and BEA JMS. Additionally, a custom adapter software development kit (SDK) is available for creation of new adapters to any environment. Most policies and bladelets used within Cisco AON understand the semantics of these protocols natively, allowing for higher fidelity and control of the interaction.
- **Protocol switching:** A Cisco AON node can act as a protocol gateway between multiple applications; for example, receiving an application message through WebSphere MQ and sending it to another application as an HTTP post. Cisco AON supports protocol translation between any combination of its supported protocols.
- **Transformation:** The open transformation architecture of Cisco AON supports both XML and non-XML transformation. Cisco AON achieves eXtensible Style Language Transformation (XSLT)–based transformation with its XSLT-based transformation engine using XSLT style sheets written or procured by the customer, allowing any combination of transformations between XML and other XML or non-XML formats. External parsers can be plugged in to facilitate reading of the non-XML format and conversion to a format consumable by the engine. In addition, custom transformations can be carried out by adding a third-party Java transformation engine.
- **Service virtualization:** Based on its ability to inspect and understand the content and context of application messages, Cisco AON can act as a proxy that provides an abstraction layer for endpoint applications and applies policies without the endpoints being aware of the intermediary. This powerful capability allows consistent, distributed policy enforcement everywhere in the network—a particularly relevant capability for distributed service-oriented applications. For example, messages can be routed according to their content by matching content elements against policy rules. Cisco AON examines message types or fields (for example, part number, account type, employee location) and sets the destination based on rules, protocol headers, or other states resulting from a previous operation. For another example, Cisco AON can do load balancing across multiple endpoints using algorithms such as Round Robin (equal distribution), Weighted Round Robin (preference for certain endpoints), and Adaptive (essentially a “best-available” service based on captured state of request or response times and latency). As for message distribution, Cisco AON supports “stickiness” to endpoints based on session recognition and management, and message distribution or “fan out” whereby a message is sent to multiple destinations simultaneously.

Application Optimization

Cisco AON takes advantage of a combination of technologies to enhance message-handling performance and improve application availability. In a typical scenario only a fraction of the network traffic flow is redirected through Cisco AON, so the vast majority of network traffic passes through as usual. For packets processed by Cisco AON, the following features are designed to minimize processing overhead and achieve enterprise-ready levels of throughput and reliability:

- **System optimization:** To speed applications that require high transaction rates, Cisco AON offers performance-optimized message processing and a fast code execution path that is particularly useful in compute-intensive operations such as content-based routing and XML schema validation. In addition, you can plug in custom functions that take advantage of the optimized execution path to meet your high-performance needs.

- **Caching and compression:** Cisco AON can cache the results of previous message inquiries based on the rules defined for a type of request or on indicators set in the response. Caching can be performed for entire messages or for certain elements of a message to reduce application response time and conserve bandwidth. Either XML and non-XML response messages or elements of a message identified and accessed through XPath can be cached. Additionally, Cisco AON can compress messages between nodes. A message policy can be set to compress the data before sending an outbound message, while on the inbound side Cisco AON automatically recognizes the message as compressed and decompresses it before further processing.
- **Availability and load balancing:** As described in the previous section, Cisco AON can sit in front of an application cluster to provide high-availability and load-balancing services to applications.

Extensibility

Built on an open, extensible architecture, Cisco AON includes a set of APIs to add new adapters and bladelets. It provides an interface to develop extensions to the base AON platform using languages such as Java and C.

- The Adapter Developer Kit (ADK) supports development of plug-in custom adapters to receive and send messages from Cisco AON.
- The Bladelet Developer Kit (BDK) supports development of custom bladelets in Java and C/C++. This capability is also available in the system optimized code execution path.

Scalability and Performance

Cisco AON is designed for high performance and scalability to address the needs of the most demanding applications. It accomplishes this through:

- **Virtual cluster:** As application message traffic increases, additional Cisco AON devices (blades or appliances) can easily be added to a WCCP (Web Cache Coordination Protocol) service group within a switch or router. Thus Cisco AON can scale horizontally and transparently to match the increased traffic.

Cisco AON Design, Configuration, and Management

Cisco AON operates as a set of distributed application and network services that span business, security, administrative, and network domains. Thus, it is important to provide a set of tools that effectively and uniformly address different aspects of configurability, manageability, and visibility of the system. Cisco AON tools include Cisco ADS and Cisco AMC.

Cisco AON Development Studio

Cisco ADS is a Windows-based tool for developers to configure how application messages are handled at run time (Figure 4). Its features include:

- Easy drag-and-drop GUI environment
- Set of preconfigured functions or bladelets that can be used to create message plans
- One-button synchronization of plans with Cisco AMC
- An ADK for creation of custom adapters and a BDK for creation of custom bladelets

Table 1 lists system requirements for Cisco ADS.

Cisco AON Management Console

Cisco AMC (Figure 5) is a Linux-based Web application with full role-based access control for centralized management of the Cisco AON system. It helps ensure consistent, up-to-date configurations across all Cisco AON devices in a distributed infrastructure. Functions include:

- Configuring and managing Cisco AON nodes
- Defining and provisioning application policies
- Key and certificate management
- Monitoring of Cisco AON node events and logs to directly interface with the Cisco AON blade operations in a switch or router

Table 2 lists system requirements for Cisco AMC, and Tables 3 and 4 list standards supported by Cisco AON. Table 5 lists the new features in Cisco AON 3.0.

Figure 4. Cisco AON Development Studio (ADS) Design-Time View

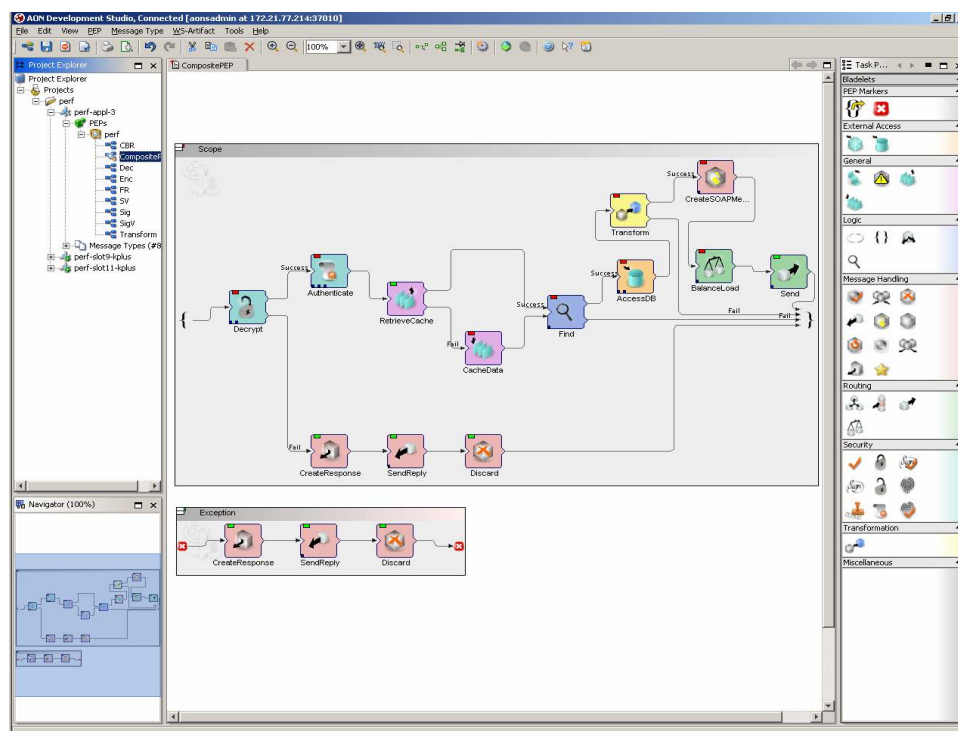


Figure 5. Cisco AON Management Console (AMC) View

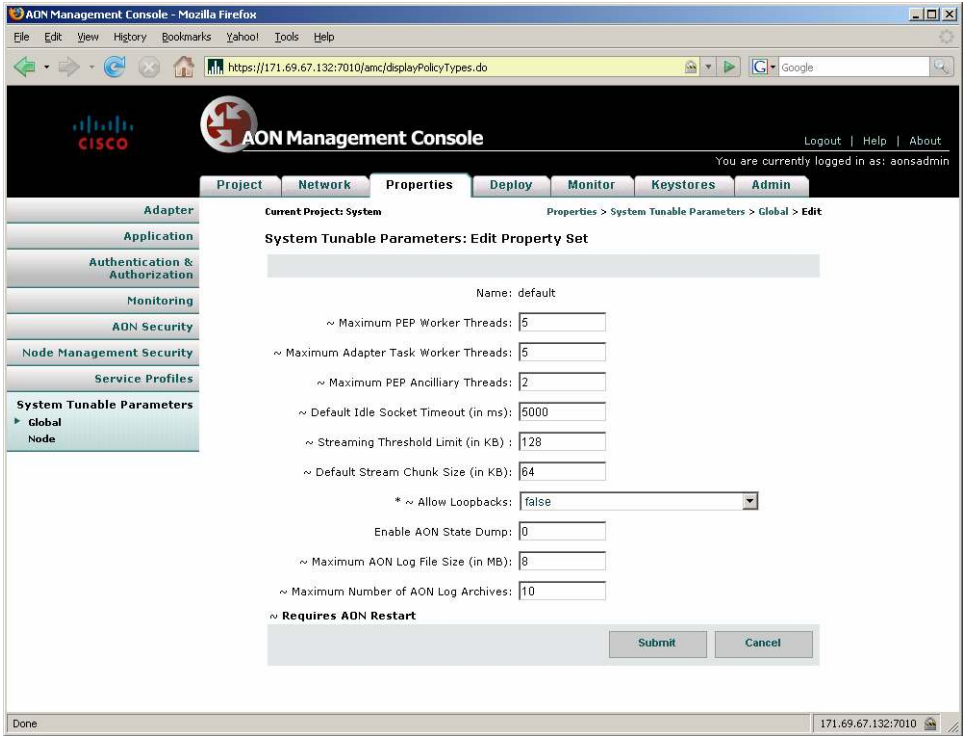


Table 1. Cisco AON Development Studio (ADS) System Requirements

Feature	Requirements
Disk space	40 GB minimum
Hardware	Single processor, Pentium IV or later
Memory	1 GB minimum (2 GB recommended)
Software	Microsoft Windows 2000 or Windows XP

Table 2. Cisco AON Management Console (AMC) System Requirements

Feature	Requirements
Disk space	40 GB minimum
Hardware	Single processor, Pentium IV or later
Memory	1 GB minimum (2 GB recommended)
Software	RedHat Enterprise Linux (RHEL) AS or ES 3.0 or later

Table 3. Cisco AON Supported Standards

Category	Standards
Transport protocols	HTTP 1.0 and 1.1, HTTPS, JMS, Tibco EMS, IBM WebSphere MQ, BEA WebLogic JMS, Progress Software Sonic MQ, FTP, SMTP, and UDP
Database	Oracle 9i (9.2), Oracle 10g, Sybase 12.5.1 and Microsoft SQL Server 2000, 2003 or 2005.
Security	3DES, AES, RSAv1.5, SHA-1, MD5, PKCS#12, MPKI, JKS, SSL3.0, and TLS 1.0
Management	Simple Network Management Protocol V2 (SNMPv2); command-line interface (CLI)
XML & Web Services	SOAP 1.1, SOAP w/ Attachments, XSLT 1.0, XPath 1.0, XSD 1.0, 1.1, XKMS, WS-I Basic Profile 1.0, WSDL 1.1

Table 4. Cisco AON Supported Trust Policies Standards

WS-SecurityPolicy Assertions	Implementation
Integrity Assertions <ul style="list-style-type: none"> SignedParts Assertions SignedElements Assertions 	✓ - Sign / Verify bladelet ✓ - Sign / Verify bladelet
Confidentiality Assertions <ul style="list-style-type: none"> EncryptedParts Assertion EncryptedElements Assertion 	✓ - Encrypt / Decrypt ✓ - Encrypt / Decrypt
Token Assertions <ul style="list-style-type: none"> UsernameToken IssuedToken X509Token KerberosToken SpnegoContextToken SAMLTOKEN 	✓ - Authenticate / Authorize ✓ - Authenticate / Authorize ✓ - Authenticate / Authorize / - Authenticate / Planning ✓ - Authenticate / Authorize ✓ - Authenticate / Authorize
Transport Security	✓ - Identity bladelet

Table 5. New Features in Cisco AON 3.0

Feature	Description
WSDL and WS-Policy import and PEP generator	Ability to import WSDL and WS-Policy documents from a file-system, or from a given HTTP URL (only clear text, not HTTPS) into the ADS and, based on this, have the ADS generate a PEP with the necessary bladelets (such as Sign, Encrypt, Send, Branch, and so on) that are required to invoke the chosen service from the WSDL and enforce the policies within the WS-Policy documents.
Create SOAP Message bladelet for callout requests	This new bladelet is similar to the existing Create Message bladelet, except that it is completely geared towards allowing the user to configure outgoing SOAP calls. The bladelet can be dragged and dropped onto the PEP when the user wishes to call out to an external Web Service. The user would then be prompted to specify a WSDL (a file system or an HTTP URL).
SAML 2.0 support	AON accepts both SAML 1.0 as well as SAML 2.0 tokens in its Identify, Verify Identity, and Authorize bladelets.
SOAP request classification and prioritization	Message type definitions now allow classification to be based on SOAP headers and body tokens like WSS username token, WSS X.509 certificate token, and WSS SAML token.
Context- and content-based routing enhancements	Enhancements to content-based routing based on sender identification in HTTP or SOAP headers, HTTP header elements (HEAD, and so on), HTTP and SOAP header information (values), SOAP header, HTTP header, source IP/port number, and context-based routing based on day, date, time.
SSL support added to BEA JMS Adapter	Processing of WebLogic JMS messages over SSL is now possible. This will guarantee message security. Both one-way SSL and two-way SSL are implemented. In one-way SSL, only the server is authenticated by the client, while for two-way SSL both client and server side authentication will be used.
HTTP pipelining support	As per HTTP 1.1 spec (RFC-2616), support is now provided for pipelining of incoming HTTP requests on persistent connections, where responses need to be sent in the same order in which the requests were received.
Data streaming support	Today, embedded adapters conform to a programming model and a set of APIs defined in the adapter SDK in order to interact correctly with the AON system. The data streaming model enhances the existing interaction to support streaming of data in discrete chunk sizes.
Syslog extended to NOTICE and DEBUG	Added support for redirecting AON logs to syslog for DEBUG and NOTICE level messages.
Multiport support on appliance	Changes have been made to enable the use of the third network interface on AON appliances.
Message order preservation	Messages may need to be delivered at the outbound in the same sequence as they were received at the inbound. A new combination of Unreliable/Ordered delivery semantics was added.
SNMP MIB metrics	A comprehensive set of SNMP MIB metrics were added as part of this release.
Notification bladelet	A new bladelet that allows the user to send a custom notification by e-mail or SNMP trap.

Microsoft SQL Server support for Log bladelet	Ability to select Microsoft SQL Server database while creating a Message Log policy in AMC has been added.
System-tunable parameters	A new policy that allows the administrator to modify system-tunable parameters such as number of threads and so on has been added.

Ordering Information

Table 6 lists the part numbers for AON 3.0 software and associated hardware.

Table 6. AON 3.0 Ordering Information

Items	Part Number	Description
Enhanced Network Module for Cisco 2800/3700/3800 series	• NME-AON-K9=	Cisco 2800/3700/3800 Series Application-Oriented Networking Enhanced Network Module
	• SW-AON-PBR-K9	Cisco AON Software 3.0 for Cisco 2800/3800 Series AON Enhanced Network Module
Cisco AON CADE 1010 Appliance	• CADE-1010-K9	Cisco ADE 1010 Application-Oriented Networking Appliance
	• SW-AON-PSMB-K9	Cisco AON Software 3.0 Platform for SMB
Cisco AON CADE 2142 Appliance	• CADE-2142-K9	Cisco ADE 2142 Application-Oriented Networking Appliance
	• SW-AON-PENT-K9	Cisco AON Software 3.0 Platform for Enterprise

For any questions related to ordering, call your Cisco account representative.

Service and Support

Cisco Services offer a flexible suite of support services designed to help maintain high-quality network performance while controlling operational costs. The services and support programs described in Table 7, Cisco SMARTnet[®] Service and Software Application Support (SAS), are available as part of the Cisco AON Service and Support solution and are available directly from Cisco and through Cisco Certified Partners.

Table 7. Cisco SMARTnet and Software Application Service and Support Programs

Service and Support	Features	Benefits
Available directly from Cisco or through Cisco Certified Partners <ul style="list-style-type: none"> • Cisco SMARTnet Service • Cisco SAS 	<ul style="list-style-type: none"> • Access to software updates and upgrades 24 hours a day • Web access to technical repositories and tools • Telephone support through the Cisco Technical Assistance Center (TAC) • Advance replacement of hardware parts (Cisco SMARTnet Service only) 	<ul style="list-style-type: none"> • Supplements existing staff • Helps ensure that functions meet needs • Mitigates risk • Helps enable proactive or expedited problem resolution • Lowers total cost of ownership (TCO) by using Cisco expertise and knowledge • Helps minimize network downtime

Cisco AON products can optionally be bundled with Cisco Advanced Services that will accelerate your time to deployment and help ensure a high-quality, reliable implementation. For more information about Cisco services, refer to [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

Software Extension Modules based on the AON platform

There are a number of Software Extension Modules based on the AON platform that are available separately. These include the following:

- [Healthcare Services Extension Module](#)
- [Financial Services Extension Module](#)
- [Secure File Transfer Extension Module](#)
- [RFID Extension Module](#)

For More Information

For more information about the Cisco AON platform, visit <http://www.cisco.com/go/aon> or contact your local Cisco account representative.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0804R)